Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 23 September 2004

Current Nationwide Threat Level is
ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS
For info click here
www.whitehouse.gov/homeland

Daily Overview

- The Transportation Security Administration has announced the deployment at three additional major airports of a new Explosives Trace Detection Document Scanner that can "sniff" passenger documents such as boarding passes and drivers' licenses for traces of explosives. (See item 5)
- The Department of Homeland Security has announced that integrated ten−print biometric identification technology is operating in every U.S. Customs and Border Protection patrol station throughout the country. (See item 9)
- The Agency for Healthcare Research and Quality has funded a new planning guide to help communities nationwide make sure that all Americans have needed drugs and vaccines in the event of a natural epidemic or bioterrorist attack. (See item 22)

DHS/IAIP Update *Fast Jump*

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *September 23, Reuters* — **Oil reserves drop for first time in five years. U.S. proven crude oil reserves fell in 2003 for the first time in five years, as energy companies replaced slightly less than 60 percent of the oil they took out of the ground, the Energy Information Administration (EIA) said on Wednesday, September 21.** The latest data show the U.S. will remain addicted to foreign oil imports for the foreseeable future. Critics have also complained

that oil companies are not spending enough of their record profits to develop more supplies. Total U.S. crude oil reserves stood at 21.891 billion barrels at end of 2003, down 3.5 percent from the year before, the Energy Department's analytical arm said. The amount of crude oil discovered last year totaled 1.232 billion barrels, 30 percent more than 2002's discoveries of 946 million barrels, the EIA said.
Source: http://www.washingtonpost.com/wp−dyn/articles/A41791−2004Sep 22.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

2. *September 22, Associated Press* — **U.S. expands military outposts. The U.S. military is expanding its network of small outposts worldwide to help fight terrorism in Middle East and African hotspots. Among the places the military already has placed or hopes to base such new "lily pads" or jumping off points: the eastern European nations of Bulgaria and Romania; a pier in Singapore; and a tiny island off the coast of West Africa.** "Freedom of action," is a term the Pentagon now uses to describe the flexibility it seeks. In short, the size, location and capabilities of the U.S. military overseas is about to undergo the most profound change since the the end of World War II and the Korean War, said Douglas Feith, the undersecretary of defense for policy, in an interview Wednesday, September 22. The Pentagon already has lined up a number of forward operating sites that have few, if any, permanent American troops. Some store U.S. war materiel, others are merely "gas−and−go" way stations. **The Navy, for its part, is developing a new approach that it calls "sea basing." It wants to build a fleet of large maritime ships capable of launching and sustaining a combat force −− either Army or Marine −− thousands of miles from shore.**
Source: http://msnbc.msn.com/id/6072771/

[Return to top]

Banking and Finance Sector

3. *September 21, Wired* — **Hacker attacks slow Authorize.Net.** Hackers have disrupted service for one of the internet's biggest credit card processors, and many online merchants are losing business while the company struggles to recover. **Since last Wednesday, September 15, Authorize.Net has been harassed repeatedly by distributed denial of service (DDoS) attacks.** The coordinated waves of internet traffic have repeatedly overwhelmed the company's servers. Authorize.Net's customers have had to improvise: Some are confirming their credit card orders over the phone, others have gone with little or no sales for nearly a week. **As of Tuesday, September 21, the attacks continued to occur.** Security experts say that there's little a company can do to defend itself against these kinds of attacks. But company officials insist they're trying. "We're actively trying to deal with it. And we're working hard to minimize

the disruptions to our merchants," Authorize.Net marketing director David Schwartz said. **The company has turned to the FBI, as well as outside consultants, for help, he added. With about 90,000 customers, Authorize.Net is one of the internet's best−known, most widely used credit card processing services, focusing mostly on smaller merchants.**
Source: http://www.wired.com/news/infostructure/0,1377,65039,00.html

4. *September 21, Asheville Citizen−Times (NC)* — **Beware of scams tied to storm damages, repairs. Criminals posing as representatives of the Federal Emergency Management Agency (FEMA) have telephoned victims of Tropical Storm Ivan in at least three Western North Carolina counties and asked for bank account information in an effort to defraud them, officials said Tuesday, September 21.** Federal, state and local officials issued warnings to residents to be vigilant against schemes designed to take advantage of those who suffered damage from the storm. Jack Heesch, a public information officer with FEMA, said the development isn't unexpected. "FEMA doesn't call people and FEMA doesn't try to get bank account information from them," he said. Hit−and−run scam artists travel to disaster areas following a hurricane, ice storm or tornado to prey on residences, according to the North Carolina Attorney General's Office. Crooked contractors cause additional financial harm by taking large deposits and then disappearing, by performing work in a shoddy manner or failing to do the work in the time expected. Terry Summey, building safety director for the city of Asheville, encourages residents to verify that their contractor or repairman has a North Carolina contractor license or a city business license.
Source: http://www.citizen−times.com/cache/article/regional/61946.sh tml

[Return to top]

Transportation Sector

5. *September 22, Transportation Security Administration* — **TSA pushes new security technology at airport passenger checkpoints.** In a significant technology advancement, **the Transportation Security Administration (TSA) on Wednesday, September 22, announced the deployment at three additional major airports of a new Explosives Trace Detection Document Scanner that can "sniff" passenger documents such as boarding passes and drivers' licenses for traces of explosives.** The airports are Los Angeles International (LAX), New York's John F. Kennedy (JFK) and Chicago's O'Hare International (ORD). "TSA is committed to deploying new explosives detection technologies to passenger security checkpoints to safeguard the traveling public," said Rear Admiral David M. Stone, USN (Ret.), Assistant Secretary of Homeland Security for TSA. The pilot program was first unveiled two weeks ago at Ronald Reagan Washington National Airport. Tests will be conducted for a minimum of 30 days at each airport. The Document Scanner analyzes samples collected by swiping the surface of a document over a collection disc and alerts the screener if explosives residue is detected. During the pilot, passengers selected for secondary screening at particular checkpoints will have their boarding passes scanned. If the Document Scanner alarms, additional screening procedures will be implemented.
Source: http://www.tsa.gov/public/display?theme=44&content=090005198 00cf9c8

6. *September 22, CNN* — **U.S. diverts plane because Cat Stevens on board.** Singer Yusuf Islam, formerly known as Cat Stevens, was taken off a diverted United Air Lines flight from

London to Washington after his Muslim name turned up on a "watch list" designed to keep terrorists from boarding flights, a Transportation Security Administration (TSA) spokesperson said. The 56−year−old Islam took that name when he became a Muslim in the 1970s. Islam, a British citizen, was being held in Bangor, ME, after Flight 919 was ordered to land there Tuesday, September 21. **A government official said Islam was on the watch list because of "known associations and financial support to organizations believed to be aiding terrorism."** The Boeing 747 had about 280 passengers and crew on board when it took off from London's Heathrow Airport, United Air Lines spokesperson Jeff Green said. The plane was met by federal agents on arrival in Bangor, where it was on the ground for about four hours before being allowed to depart, Green said. **According to a TSA spokesperson, Islam made it through pre−screening by United Air Lines and was given a boarding pass. But after the flight took off, the U.S. Customs and Border Protection agency discovered his name was on a watch list.**
Source: http://www.cnn.com/2004/US/09/22/plane.diverted.stevens/inde x.html

7. *September 22, Transportation Topics News* — **Some states not ready for next fingerprint deadline.** With the federal deadline fast approaching for states to begin fingerprinting hazardous materials drivers, industry officials said it may already be too late for all states to launch the program on time. States are supposed to start using fingerprints by January 31, 2005, to check new and renewing applicants for Hazmat−hauling endorsements to commercial driver licenses (CDL), under a regulation the Transportation Security Administration (TSA) issued last spring. **However, in many cases the people at the state and local level who process CDLs needed new authority in state law to put fingerprinting into effect, and state agencies have said they needed funds to cover the added equipment and training costs.** Cliff Harvison, president of the National Tank Truck Carriers, said last week that many states “may get caught in a time warp” because their legislative schedules might not allow them to meet the TSA deadline.
Source: http://www.ttnews.com/members/topnews/0011934.html

8. *September 21, Department of Transportation* — **DOT announces funds to repair Airport, I−10 bridges.** The federal government will spend almost $4.5 million to help fund initial repairs to the Pensacola Regional Airport and a pair of bridges that carry Interstate 10 across Escambia Bay left damaged by Hurricane Ivan, U.S. Department of Transportation (DOT) Secretary Norman Y. Mineta announced on Tuesday, September 21, during a visit to both sites. **Mineta announced that almost $2.5 million would be available for airport repairs and another $2 million would be available for work on the bridges. “The damage done by Hurricane Ivan to Pensacola’s bridges, roads and airport reminds us how much we rely on our transportation network and how important it is to our economy and quality of life,”** he said during a news conference in the empty airport terminal. During his visit, Mineta saw how Ivan’s powerful winds knocked down terminal walls and lifted roofs from buildings. He also visited temporary radar control facilities brought in for air traffic controllers displaced when the storm destroyed their offices.
Source: http://www.dot.gov/affairs/dot17704.htm

9. *September 21, Department of Homeland Security* — **DHS announces biometric identification system operational at border patrol stations.** The Department of Homeland Security (DHS) in a joint effort with the Department of Justice announced on Tuesday, September 21, that

integrated ten−print biometric identification technology is operating in every U.S. Customs and Border Protection (CBP) Border Patrol station throughout the country. **The newly advanced capability allows CBP Border Patrol agents to simultaneously search the FBI's fingerprint database. The Integrated Automated Fingerprint Identification System (IAFIS) and DHS's Automated Biometric Identification System (IDENT) provide rapid identification of individuals with outstanding criminal warrants through electronic comparison of ten−print digital finger scans against a vast nationwide database of previously captured fingerprints.** This week, the IDENT/IAFIS program is fully operational within all 148 Border Patrol stations and is in the process of being deployed to all the ports of entry nationwide, exceeding DHS's prior commitment by bringing the deployment instead to 100% of Border Patrol stations months ahead of schedule. All 115 air and sea ports of entry and the busiest 50 land border ports of entry will have this capability by November 15, 2004. In 2005 remaining ports of entry and all Immigration and Customs Enforcement (ICE) field locations will plan for deployment.
Source: http://www.dhs.gov/dhspublic/display?content=4030

10. *September 21, Department of Homeland Security* — **New approach to border security shows results.** Six months after launching an innovative multi−agency enforcement initiative at the Arizona Border, the Department of Homeland Security (DHS) can point to steady progress toward stemming illegal immigration into the Southwest United States, Asa Hutchinson, Under Secretary for Border and Transportation Security (BTS), announced on Tuesday, September 21. Since DHS kicked off the Arizona Border Control (ABC) initiative March 16, 2004, agents have made more than 351,700 illegal immigrant apprehensions at the Arizona border −− evidence of substantial progress at securing the border against illegal incursions. Prosecutions of human smuggling organizations, another key indicator, have increased by 68 As part of the ABC initiative, DHS has dedicated additional technology and tools to border security. **Unmanned aerial vehicles (UAVs) were incorporated to increase border surveillance of illegal activities. Two additional helicopters have been permanently reassigned to boost air capability along the 375−mile border. In addition, the Air and Marine Operations division of U.S. Immigration and Customs Enforcement (ICE) provides additional air surveillance, interdiction and law enforcement support.** For additional information refer to the DHS Fact Sheet: http://www.dhs.gov/dhspublic/display?content=4029
Source: http://www.dhs.gov/dhspublic/display?content=4028

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

11. *September 22, Canadian Press* — **Bird flu outbreak reported in Cambodia. A farm near the Cambodian capital was closed after about 2,300 chickens died of Avian flu −− apparently the first cases of the disease in the country following an epidemic in Asia**

earlier this year. The remaining 2,200 birds at the farm were destroyed Wednesday, September 22. Testing by the Pasteur Institute in Phnom Penh confirmed the bird flu strain of H5N1, said Som Sin, head of the local agriculture office. The earlier outbreak of bird flu killed or forced the slaughter of more than 100 million birds across 10 Asian countries. Avian flu was found in 12 areas of Cambodia during the epidemic. There were no human victims in the country, but more than 30,000 chickens, ducks, and other fowl were slaughtered to prevent the disease from spreading.
Source: http://www.canada.com/health/story.html?id=81b3f40a−aef7−4d06−bebb−5001a63a9a67

12. *September 21, CIDRAP News* — **Links between human and animal disease surveillance growing.** State Public Health Veterinarian Mira Leslie hopes to greatly expand Washington's disease surveillance network October 1 when she speaks at a statewide veterinary meeting. She will explain how a $75,000 grant from the Centers for Disease Control and Prevention (CDC) lets veterinarians test domestic animals for plague and tularemia at a university diagnostic lab. It's one prong of a statewide biosurveillance project that will include screening of wild mammals as well as pets. **The grant has several goals: gathering baseline data for understanding zoonotic diseases that could be used as biological weapons, identifying emerging infections, improving communication between vets and public health workers, and paying for diagnostic testing, Leslie said.** Leslie expects to receive samples from healthy and sick outdoor pets from vets in each of 10 regions in the state, allowing health officials to map the distribution of exposure to endemic diseases such as plague and tularemia. In addition to providing routine samples, veterinarians as well as wildlife biologists and other experts can submit the bodies of domestic pets and wild animals with suspicious signs for full necropsy. The Washington project is one example of a growing national and international movement to link the monitoring of human and animal diseases.
Source: http://www.cidrap.umn.edu/cidrap/content/bt/bioprep/news/sep t2104vetspub_rev.html

[Return to top]

Food Sector

13. *September 21, Food Navigator* — **Sweden beats salmonella.** The salmonella bacteria is a major problem in most countries across the globe and can be carried in eggs, poultry and other meats, raw milk, and chocolate. Representatives from the U.S. Department of Agriculture (USDA) have been in Sweden to study the methods in detail. "Sweden has practically managed to eliminate salmonella from its chicken breeding. Now, we want to find out how we in the U.S. can use parts of the Swedish method to prevent salmonella" said Stan Bailey of the USDA. In North America today, salmonella can be found in 10 to 35 percent of the chickens. So far, efforts to fight salmonella have been concentrated on latter parts of the production chain, using heating and radiation. **The Swedish method moves the control points backwards in the production chain, including the egg production site, as well as strong focus on hygiene−related matters.**
Source: http://www.foodnavigator.com/news/news−NG.asp?n=54849−sweden−beats−salmonella

14.

September 20, Food Production Daily — **Oregano−cranberry mix cuts Listeria. Scientists from the department of food science at the University of Massachusetts say that cranberry and oregano extracts combined with lactic acid may inhibit the growth of the food pathogen Listeria monocytogenes in meat and fish.** Listeria is a hardy bacterium capable of growing in refrigerated temperatures making it very difficult to control. "Oregano and cranberry, useful botanicals generally regarded as safe for food flavouring and as functional ingredients are known for their antimicrobial activity linked to the phenolic moiety [specific segment of a molecule] and therefore are suitable as antimicrobial natural extracts when effectively combined with lactic acid," said the researchers. The scientists said that antimicrobial activity increased when oregano and cranberry extracts were mixed at a ratio of 75 percent oregano and 25 per centcranberry with 0.1 mg of phenolic per disk. Their findings are reported in the journal of Applied and Environmental Microbiology.
Source: http://www.foodproductiondaily.com/news/news−NG.asp?n=54803−oregano−cranberry−mix

[Return to top]

Water Sector

15. *September 22, Richmond Times Dispatch (VA)* — **Updating water system proves slippery.** A year after Hurricane Isabel left most of the Richmond, VA, area without safe drinking water for days, city officials haven't decided whether they can afford to make the system less vulnerable to the loss of electrical power. **City officials, however, are now taking a closer look at a plan that would install backup power for the water treatment plant and 14 pumping stations that move water to customers' faucets. They're also taking a broader look at whether the system needs a complete makeover, possibly with fewer, bigger pump stations. Such a model would require fewer backup generators should another disaster strike, and it could operate more efficiently.** Isabel's destructive power exposed vulnerabilities in public water systems throughout Virginia. The storm knocked out power at 100 water pumping stations across the state and forced health officials to warn customers of 237 water systems to boil water before drinking it. Two big public water systems, in Richmond and Fairfax County, both shut down because they didn't have enough backup power to pump safe, purified water to customers. The state's biggest water system, the Fairfax County Water Authority, has committed to a $60 million plan to install backup generation at both of its water treatment plants and its two most critical pumping stations, as well as expanding its capacity for storing treated water.
Source: http://www.timesdispatch.com/servlet/Satellite?pagename=RTD%2FMGArticle%2FRTD_BasicArticle&c=MGArticle&cid=1031778089954&path=!news&s=1045855934842

16. *September 22, Science and Development Network* — **WHO updates water safety guidelines.** The World Health Organization (WHO) has issued new safety guidelines for drinking water that put the emphasis on prevention of waterborne disease rather than responses to outbreaks. **Currently, water sanitation relies largely on testing water samples for chemical and biological contaminants, but this often means that pollutants are identified long after the water has been consumed. Instead, says the WHO, regulators should ensure water quality by protecting water sources and controlling treatment processes from source to tap.** The WHO guidelines will help reinforce one of the UN Millennium Development Goals, which is to

halve the number of people −− currently 2.6 billion, mostly in developing countries −− without access to safe water and basic sanitation by 2015. The guidelines can be found at: http://www.who.int/water_sanitation_health/dwq/guidelines/en / Source: http://www.scidev.net/news/index.cfm?fuseaction=readnews&itemid=1615&language=1

[Return to top]

Public Health Sector

17. *September 22, Associated Press* — **Proposal aimed at reducing mad cow risk. The government is taking steps to reduce the already minimal risk of mad cow tainted components ending up in childhood vaccines and other medications.** Pharmaceuticals regulated by the Food and Drug Administration (FDA), including human vaccines and animal drugs used on farms, routinely use cow products in their manufacture. William Egan, FDA acting director in the office of vaccine research and review, told pharmaceutical representatives that the new rule is aimed at reducing even further mad cow risk in human and animal drugs. He did not offer specifics. **There have been no reported cases of mad cow transmitted by medications. Dozens of people, however, were infected with Creutzfeldt−Jakob disease, related to the human form of mad cow, by taking tainted human growth hormone between 1963 and 1985, according to the National Institutes of Health.** The method of manufacturing the growth hormone was changed in response to that risk. In July 2000, the FDA told manufacturers to replace products in their vaccines derived from cows born, raised and slaughtered in countries with confirmed mad cow cases. The FDA's Egan said the agency has not yet decided whether manufacturers will have to replace American and Canadian cow products routinely used in vaccine manufacturing.
Source: http://www.miami.com/mld/miamiherald/living/health/9727665.h tm?1c

18. *September 22, Associated Press* — **Whooping cough on the rise in New York. The number of New Yorkers affected by the highly contagious respiratory illness passed the 1,000 mark for the second straight year, prompting health officials to step up efforts to stave off the disease.** Earlier this year, the state Health Department posted a bulletin to community health departments and health care providers about the recent trend. A similar alert was sent in June to directors and nurses at summer camps. Now with the fall school year underway, the focus is shifting to school nurses and teachers to be on the alert. **New York is among seven states that currently do not require school−age children to be vaccinated against whooping cough.** Starting next year, babies born after January 1 would be required to be vaccinated against whooping cough before they enter school or day care, under a new law. **So far this year, there were 1,448 confirmed cases of whooping cough, up from 388 in 2000. The average is 300 cases annually.** Health experts say a number of factors may be responsible for the spike in whooping cough cases in recent years, a trend that is mirrored nationwide, although they have been unable to pinpoint an exact cause.
Source: http://www.newsday.com/news/local/wire/ny−bc−ny−−whoopingcough0922sep22,0,6987317.story?coll=ny−ap−regional−wire

19. *September 22, PhysOrg* — **Nanowires capable of detecting viruses. Harvard University scientists have found that ultra−thin silicon wires can be used to electrically detect the**

presence of single viruses, in real time, with near−perfect selectivity. These nanowire detectors can also differentiate among viruses with great precision, suggesting that the technique could be scaled up to create miniature arrays easily capable of sensing thousands of different viruses. The researchers merged nanowires conducting a small current with antibody receptors for certain key domains of viruses −− such as agglutinin in the influenza A virus. When an individual virus came into contact with a receptor, it sparked a momentary, telltale change in conductance that gave a clear indication of the virus's presence. Simultaneous electrical and optical measurements using fluorescently labeled influenza A confirmed that these conductance changes corresponded to binding and unbinding of single viruses from nanowire devices. In addition to influenza A, the researchers tested nanowire arrays outfitted with receptors specific to paramyxovirus and adenovirus. The researchers found the detectors could differentiate among the three viruses both because of the specific receptors used to snag them and because each virus binds to its receptor for a characteristic length of time before dislodging −− leaving only a minuscule risk of a false positive reading.
Source: http://www.physorg.com/news1262.html

20. *September 21, Associated Press* — **Government to buy bird flu vaccine. The government plans to buy two million doses of an experimental vaccine against the bird flu to stockpile in case the virus one day sparks a large outbreak in people. The $13 million purchase is part of the effort to prepare for the next flu pandemic, the Department of Health and Human Services (HHS).** Three flu pandemics have occurred in the last century, the worst the 1918 outbreak that killed more than half a million Americans and 20 million people worldwide. Flu specialists say it's only a matter of time before another such worldwide outbreak strikes, and there's concern that the recurring bird flu in Asia could be the trigger if it were to mutate to spread easily among people. The new vaccine is designed to match the H5N1 bird flu strain that has killed 28 people in Asia this year, as well as infected millions of poultry. Testing of the experimental vaccine should begin this year, HHS officials said.
Source: http://www.nctimes.com/articles/2004/09/22/special_reports/science_technology/15_36_209_21_04.txt

21. *September 21, Vancouver Sun (Canada)* — **Sickness strikes cruise ship. A total of 276 passengers and crew became ill from suspected outbreaks of the Norwalk virus aboard the cruise ship Sun Princess on its final three Alaska voyages, according to Health Canada.** On Monday the ship −− empty of passengers −− left Vancouver, Canada, for San Francisco, CA, at the end of the cruising season in British Columbia and Alaskan waters after a quick examination by federal officials, said Kevin Carlise, public health manager with Health Canada. When the ship docked in Vancouver September 6, after leaving Whittier, Alaska, 11 passengers were reported suffering vomiting and diarrhea −− symptoms of norovirus, also known as the Norwalk virus, he said. The ship normally carries approximately 2,000 passengers and 800 crew. When the Sun Princess turned around September 6 and headed back to Alaska there were 145 passengers and five crew who came down ill with Norwalk symptoms during the voyage. The ship then left Alaska with a new intake of passengers and when it arrived in Vancouver, Monday, September 20, 101 passengers and 14 crew were reported sick.
Source: http://www.canada.com/vancouver/vancouversun/news/story.html?id=895172c4−e7dd−4e6d−ab02−f548ede02f4c

22.

September 20, Agency for Healthcare Research and Quality — **Preparing for vaccine and drug dispensing. A new planning guide funded by the Agency for Healthcare Research and Quality is designed to help communities nationwide make sure that all Americans have needed drugs and vaccines in the event of a natural epidemic or bioterrorist attack.** Developed by a team of researchers in the Department of Public Health at Weill Medical College of Cornell University and New York−Presbyterian Hospital, the guide complements the Strategic National Stockpile guidebook prepared by the Centers for Disease Control and Prevention, which includes a chapter on dispensing medications and vaccines. The new guide, Community−Based Mass Prophylaxis: A Planning Guide for Public Health Preparedness, is designed to help State, county, and local officials meet Federal requirements for a public health emergency. **The guide provides a framework for understanding the components of epidemic outbreak response (surveillance, stockpiling, distribution, dispensing, and followup care) and the planning and conduct of dispensing operations using specially designated dispensing clinics.** The guide applies these concepts to develop model pill−dispensing and vaccination clinics run on the Bioterrorism and Epidemic Outbreak Model (BERM), a computer staffing model that can be customized to meet local community needs. The guide can be found at: http://www.ahrq.gov/research/cbmprophyl/cbmpro.htm
Source: http://www.medicalnewstoday.com/medicalnews.php?newsid=13835

[Return to top]

Government Sector

23. *September 20, Federal Computer Week* — **DHS advances information sharing. To encourage better information sharing, the Department of Homeland Security (DHS) on Monday, September 20, awarded nine million dollars for 12 demonstration projects in its Information Technology and Evaluation Program (ITEP) that will help show how to remove barriers to sharing information.** "One of the important lessons our nation learned in the aftermath of the [September 11, 2001] terrorist attacks was that we had to do a better job of sharing information at all levels of government, as well as with the private sector," said C. Suzanne Mencer, director of DHS' Office for Domestic Preparedness. Some of programs selected include: Secure Homeland Access and Reporting Environment, Extensible Emergency Operations Center, Data Coordination Homeland Security Module, Emergency Geographic Information Network, Criminal Justice Information Systems Integration and Sharing Pilot, and Port Security Communications Network.
Source: http://www.fcw.com/geb/articles/2004/0920/web−info−09−20−04. asp

[Return to top]

Emergency Services Sector

24. *September 21, eWeek* — **Enhanced 911 service for wireless hits standardization logjam.** Claims by wireless carriers that some basic characteristics about their network performance are proprietary threatens to keep emergency workers from aiding victims in a timely manner, said speakers at a panel in the Hart Senate Office Building in Washington, DC, on Tuesday, September 21. The panel, presented by the E9−1−1 Institute, reported on the state of Enhanced

911 services for wireless users. Industry representatives said that efforts to meet Federal Communications Commission requirements for E911 support have been hampered by a lack of specificity in the commission's rules. **Perhaps the worst problem, however, is the refusal of wireless carriers to divulge the accuracy of the position information provided to emergency services.** "They're really worried that the press will get the information and use it," Nancy Pollock, executive director of the Metro 911 Board for Minneapolis−St. Paul, MN, told the panel. When a wireless caller makes an emergency call, the call is supposed to be transferred to the emergency operations center in the jurisdiction where the caller is located. **But when the actual location isn't known, then the response must be much larger because the caller must be located before they can be helped. Responders have no way to know whether the caller is located at a specific intersection, for example, or simply that they're in some general area of town.**
Source: http://www.eweek.com/article2/0,1759,1649208,00.asp

[Return to top]

Information Technology and Telecommunications Sector

25. *September 21, SecurityTracker* — **Windows XP Service Pack 2 firewall configuration error exposes file and print sharing to remote users.** A vulnerability was reported in Windows XP Service Pack 2 (SP2). It is reported that when XP SP2 is installed on a certain configuration, a remote user can access the shared files and printers on the target system, even though the Windows XP firewall is enabled. No vendor solution is currently available. Original advisory and workaround is available at: http://www.pcwelt.de/know−how/extras/103039/
Source: http://www.securitytracker.com/alerts/2004/Sep/1011374.html

26. *September 21, The Register* — **Do−It−Yourself Wi−Fi causes security headache.** Frustrated employees are taking IT into their own hands by installing Do−It−Yourself (DIY) Wi−Fi access points (WAPs) in their offices while their IT departments don't even notice, according to Gartner research. **A rogue access point can leave an organization's network wide open and once on the network, an unauthorized user could go undetected.** Monitoring WLAN traffic "in the air" is the most effective means of detecting unauthorised systems, said John Girard, Gartner research vice−president. The least expensive, but least effective, way of achieving this is to buy a handheld wireless sniffer and patrol the perimeter of the organization's network. The most expensive, but most secure, method is to install a separate set of wireless intrusion detection sensors.
Source: http://www.theregister.co.uk/2004/09/21/diy_wifi_security/

27. *September 21, CNET News.com* — **Academics get $12 million NSF grant for Net security centers. The National Science Foundation (NSF) announced Tuesday, September 21, that it has granted more than $12 million to academic researchers for the creation of two centers to investigate infectious code and study the Internet's ecology.** The funds set aside for the centers are part of the NSF's Cyber Trust program, through which the foundation has granted a total of $30 million to 33 projects focused on researching ways to provide better information security. The Center for Internet Epidemiology and Defenses, or the CIED, will work to understand how digital diseases such as worms and viruses spread across the Internet, and how epidemics can be defeated. The Security Through Interaction Modeling, STIM, Center

will draw parallels with nature's ecology to understand the complex interaction between machines, humans and cyberattacks.
Source: http://zdnet.com.com/Academics+get+NSF+grant+for+Net+security+centers/2100−1105_2−5376474.html

28. *September 21, internetnews.com* — **Security fears still blocking WLAN adoption.** Despite the best efforts of the Wi−Fi industry to assure companies wireless networking is safe in the workplace, a new survey of executives finds security remains the leading barrier to WLAN adoption. **Although 84 percent of companies have not had their WLAN breached, "security is the top barrier, cited by nearly half of all companies" as the reason they are not deploying or expanding Wi−Fi networks, according to a report by Jupiter Research.** "The percentage of companies spending more than $10,000 annually [on WLAN deployments] will grow from 26 percent in 2003 to 35 percent in 2004," said Jupiter research director Julie Ask. Number−wise, growth in WLAN deployments is occurring in small businesses, while budget increases are being seen with larger companies. "The primary driver behind deployments today is employee demand," said Ask. More employees are using wireless at home, and after getting used to the idea, they are demanding it in the workplace.
Source: http://www.internetnews.com/wireless/article.php/3410951

29. *September 21, IDG News Service* — **When outsourcing, cultural differences may affect security.** When it comes to outsourcing IT operations to countries such as India and China, companies often focus on slashing costs and gaining productivity but fail to take into account cultural differences that may affect their security, according to experts attending the Gartner IT Security Summit in London this week. **At issue is not so much the security that outsourcing service providers use to protect companies' systems −− such as firewalls and data backup −− as it is the cultural differences, said Gartner India research vice president Partha Iyengar.** For instance, standards of privacy are often looser in India because it's a close−knit society where, say, reading someone else's e−mail wouldn't be considered much of an intrusion. This more relaxed attitude toward privacy could have serious consequences when it comes to protecting corporate data. Companies that outsource operations overseas are advised to train local staff to adhere to the company's global privacy standards and to check into the risk of government interception of sensitive confidential information.
Source: http://www.computerworld.com/managementtopics/outsourcing/story/0,10801,96074,00.html

30. *September 21, Reuters (Monterrey, Mexico)* — **Mexican churches wage high−tech war on cell phones.** Some Mexican churches are using state−of−the−art technology developed by Israeli electronic warfare experts to silence cell phones that ring during mass, church officials said on Tuesday, September 21. Four churches in the northern city of Monterrey, which lies some two hours by car south of the Texas border, are using equipment made by an Israeli telecoms equipment firm to block incoming calls during services. **The Tel Aviv−based company was set up in 1998 by former military and defense industry specialists to develop mobile telephone jamming systems, mainly for the security industry**. "Now we are getting calls from all over the country to see how it can be installed," said Bulmaro Carranza, a caretaker at one of the churches.
Source: http://story.news.yahoo.com/news?tmpl=story2&u=/nm/20040921/tc_nm/life_mexico_cellphones_dc

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: Microsoft released a new security bulletin detailing critical vulnerabilities in the way it handles JPEG graphics. More information can be found here: http://www.microsoft.com/technet/security/bulletin/ms04−028. mspx.

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 135 (epmap), 1434 (ms−sql−m), 137 (netbios−ns), 9898 (dabber), 5554 (sasser−ftp), 1433 (ms−sql−s), 1023 (Reserved), 1026 (nterm), 1027 (icq) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP Web page (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Alerts − Advisories and Information Bulletins: DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues.

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports.

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

DHS/IAIP Disclaimer